



Information and Technology for Better Decision Making

Evolution of the DoD CAC Program

Prepared for

NIST

Presented by

Mary Dixon

Director, Access Card Office



July 8, 2003

Background

November 10, 1999

MEMO FROM:

Dr. John Hamre

(Deputy Secretary of Defense)

Create a Common Access Card!

Requirements for Convergence of Three Separate Initiatives

Smart Card

- Pilot Studies
- Business Process Re-engineering
- No \$

E-Business

- Non-repudiation for digital signatures

PKI

- Hardware token

**Common Access Card
(CAC)**

CAC Attributes

- **Barcode**
 - **Code 39 barcode**
 - **Two-dimensional PDF 417 barcode**
- **Magnetic stripe**
- **Integrated Circuit Chip (ICC)**
- **Digital photograph**

Current Status

Card Issuance

- Over 2.83 M cards issued
- Issuing between 10-14,000 cards per day
- 1,500 issuance workstations issuing in 15+ countries worldwide
- 150,000 + workstations with logical access/log-on

Next Generation Testing

- 64K chip
- Contactless technologies (14443)
- Biometrics

Its Evolution not Revolution...

Application Strategy

Data Centric - focus of pilots



PKI

Web Centric - focus of future

- Eliminates issue - data synchronization
- Reduces rush to and expense of higher capacity cards
- Mitigates warfighter concerns over data availability to captor
- Mitigates card holders' concerns over privacy
- Must balance with communications availability

Focus on User Assistance

- CAC PIN Reset (CPR) – Army/DMDC developed application
- User Maintenance Portal (UMP)/Post Issuance Portal (PIP) – Web-centric approach to adding applications to the CAC
- Contractor Verification System (CVS) – Improved identity management for contractors
- Integration Logistics Portal (ILP) – Automated tool for inventory and logistic management of CAC cardstock
- Developers Kits

Moves card maintenance as close to user's desktops as possible



Two Components of DoD Identity Management

(Defense Cross-credential Identification System (DCIS) Proof of Concept)

DoD National Visitors Center

Authenticate

DoD **ID Credential** holders
at DoD bases and facilities
for physical access

DoD Cross-Credentialing

Authenticate

Federated Commercial and
government **ID Credentials**
Holders within DoD
and DoD ID Credentials
holders at federated facilities
and facilities

Features:

- Secure Web-based access within DoD and between Partners
- Signed delivery of authentication data including biometrics
- Trust server can be scaled to add federated partners quickly
- Standards based using signed XML

Future Enhancements/Testing

- **Central issuance**
- **RAPIDS ATM**
- **Applet changes (Access Control)**
- **64K**
- **Contactless**
- **Biometrics**

Applications

- PKI authentication, encryption, digital signatures
- Defense Travel System (DTS)
- Voting Over the Internet (VOI)
- Reserve training
 - Attendance
 - Backend to pay
- Manifesting
- Dining facilities

** More applications being developed/tested*

**As DoD Identity Management Systems
Advance, so Must...**

Interoperability/Standards

- GSC-IS is a BIG step for contact/contactless smart cards
- Movement to ISO would be a GIANT step
- Next we need to move the biometrics industry in the same direction

NIST IS CRITICAL!

Supporting Infrastructure Vendors Need to Join the March Towards Interoperability

- **Operating systems vendors**
- **Reader industry**
 - **Contact**
 - **Contactless**
- **PDA's**
- **Point of sale (POS) terminals**
- **Computer vendors**
- **Others**

Why is This Important?

- **Can reduce our costs**
- **Designs can increase market volume**
- **Identity management is a critical function**
- **Technology can make it happen**
- **Standards/interoperability make all of this affordable**

Standards Based

A common policy on identity proofing, interoperability requirements and technology standards for physical/logical access needs to be defined

- **Will this credential be able to be read outside of your facility, campus, building, room?**
- **Should you care?**
- **Multiple identity credentials vs. one identity credential**
- **Improve security**

****Affordability/Widespread Implementations****

Questions?

Mary Dixon

(703) 696-7396

dixonmm@osd.pentagon.mil